Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.025505
Article

Tech Science Press

Discrete GWO Optimized Data Aggregation for Reducing Transmission Rate in IoT

S. Siamala Devi[1], K. Venkatachalam[2], Yunyoung Nam[3,*] and Mohamed Abouhawwash[4,5]

[1]Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, 641042, India
[2]Department of Applied Cybernetics, Faculty of Science, University of Hradec Králové, Hradec Králové, 50003, Czech Republic
[3]Department of Computer Science and Engineering, Soonchunhyang University, Asan, 31538, Korea
[4]Department of Mathematics, Faculty of Science, Mansoura University, Mansoura, 35516, Egypt
[5]Department of Computational Mathematics, Science, and Engineering (CMSE), Michigan State University, East Lansing, MI, 48824, USA
*Corresponding Author: Yunyoung Nam. Email: ynam@sch.ac.kr

Received: 26 November 2021; Accepted: 11 January 2022

Abstract: The conventional hospital environment is transformed into digital transformation that focuses on patient centric remote approach through advanced technologies. Early diagnosis of many diseases will improve the patient life. The cost of health care systems is reduced due to the use of advanced technologies such as Internet of Things (IoT), Wireless Sensor Networks (WSN), Embedded systems, Deep learning approaches and Optimization and aggregation methods. The data generated through these technologies will demand the bandwidth, data rate, latency of the network. In this proposed work, efficient discrete grey wolf optimization (DGWO) based data aggregation scheme using Elliptic curve Elgamal with Message Authentication code (ECEMAC) has been used to aggregate the parameters generated from the wearable sensor devices of the patient. The nodes that are far away from edge node will forward the data to its neighbor cluster head using DGWO. Aggregation scheme will reduce the number of transmissions over the network. The aggregated data are preprocessed at edge node to remove the noise for better diagnosis. Edge node will reduce the overhead of cloud server. The aggregated data are forward to cloud server for central storage and diagnosis. This proposed smart diagnosis will reduce the transmission cost through aggregation scheme which will reduce the energy of the system. Energy cost for proposed system for 300 nodes is $0.34 \mu J$. Various energy cost of existing approaches such as secure privacy preserving data aggregation scheme (SPPDA), concealed data aggregation scheme for multiple application (CDAMA) and secure aggregation scheme (ASAS) are 1.3 μJ, 0.81 μJ and 0.51 μJ respectively. The optimization approaches and encryption method will ensure the data privacy.

Keywords: Discrete grey wolf optimization; data aggregation; cloud computing; IoT; WSN; smart healthcare; elliptic curve elgamal; energy optimization

1 Introduction

Evolution of IoT and digital technologies makes the healthcare monitoring as effective and efficient for diagnosing and real time monitoring. The data generated from these devices are huge and processing is also still a challenging task [1]. Intelligent sensor with IoT plays a vital role in the field of healthcare, agriculture, city, transportation, and industry [2]. To collect the patient health parameters such as blood glucose level, heart rate, blood pressure etc., IoT sensors are used [3]. These IoT sensor devices gather the information and transmit to cloud server for processing [4,5]. This network ensures the security of the patient data and process to provide the diagnosis result in case of emergency scenario [6]. An Anonymous and Secure Aggregation Scheme (ASAS) [7] proposed pseudonyms to protect the nodes identity. To protect the data integrity, homomorphic encryption is used. This method reduces the bandwidth utilization but due to redundant data transmission, computational cost and communication cost are increased. EHDA (Efficient health data aggregation) method [8] provides smart nodes with secure communication. Aggregate node (AN) use message receiving method for aggregation on compressed data received from smart sensor nodes. Fog node (FN) employs message receiving algorithm and decrypt the aggregated data for analysis. The contribution of the proposed work is as follows:

- In IoT wearable sensor network, rather than each node sending data to cloud centre, data are aggregated by the aggregator node which will then forward the aggregated data to cloud server through edge node. Due to this the bandwidth, network delay and number of transmissions are effectively utilized
- Each IoT sensor device encrypt the data using elliptic curve elgamal (ECE) and Calculate media access control (MAC) address for each key. This encrypted data are communicated to aggregator node.
- Aggregators add all the encrypted data using XOR with minimum alveolar conMAC. And send this information of aggregated data with MAC to edge server.
- AN nearer to edge node can send the aggregated data directly to the edge server. AN which placed far away from the edge server can communicate to its neighbor AN for data transmission. The neighbor AN can be find using efficient searching approach called Discrete GWO.
- Edge servers decrypt the data and done its local processing and transmit to cloud server for analysis.

Remaining section of this paper is as follows: Section 2 discusses about the related work. Section 3 proposed an efficient scheme for data aggregation and analysis. Section 4 discusses about the simulated results and evaluation and Section 5 concludes the proposed work with future directions.

2 Related Works

The recent research related to data aggregation schemes are listed in Tab. 1.

The work describes about cryptographic technique for securing IoMT network. They used Rivest chiper and elliptical curve digital signature algorithm with secure hashing for protecting medical data user. it strengthens the health care but number of transmissions is higher which increases the communication cost of the network. discuss about IoT in industrial application. The industrial data is transferred time to time were communication cost will be hiked. discusses about secured IoT and importance IoT in wireless networks. But they are lagging in reducing number of transmissions at a time. This problem highly focused in our paper by data aggregation technique.

Table 1: Literatures related to data aggregation and health care application

Author	Methods used	Description
Zhu et al. [9]	bilinear pairing cryptosystem	privacy preserved aggregation method for WBAN using bilinear pairing cryptosystem for data aggregation
He et al. [10]	Two data addictive aggregation method	One scheme based on clustering protocol to achieve private data aggregation and another scheme based on slicing protocol with the property of addition.
Farahani et al. [11]	Review related to fog-based data aggregation schemes.	Discussed about the challenges and issues related to data aggregation via fog node and cloud. In terms of scalability, privacy and security, it discusses the case study to point out the essential for healthcare monitoring
Gosman et al. [12]	Privacy preserving aggregation based on symmetric cryptography.	They developed the data aggregation scheme for smart transport system
Azeem et al. [13]	secure message aggregation (SMA) and secure message decryption (SMD)	efficient fog-oriented data aggregation scheme for IoMT. This model used secure message aggregation (SMA) and secure message decryption (SMD) to ensure the security and integrity.
Lin et al. [14]	CDAMA for multi-application	Ciphertext from various applications are aggregated as one. Base station can extract the ciphertext of relevant application using the respective key. This method is not suited for WSN with large number of clusters.
Ullah et al. [15]	Survey about secure data transmission and data collection for fog-based healthcare architecture	discussed about fog based efficient and reliable data collection schemes for smart city, smart grid and smart vehicle
Chen et al. [16]	Two recoverable CDA scheme called RCDA-HOMO and RCDA-HETE for heterogeneous network	This will allow the base station to recover the data generated by the sensing devices and also check the integrity of the real data. due to the base station perform the pairing computation, this method elucidates more computation overhead.
Salman et al. [17]	Particle Swarm Optimization (PSO)	PSO has been used here for task assignment problem to reduce the total execution time compared with GA.
Shim et al. [18]	EC-EG HE schemes and a signature method	This method ensures the data confidentiality, integrity, false data filtering and authorized aggregation. But it lacks in high computation and communication overhead. Public key sharing at base station may leads DoS attacks.

(Continued)

Table 1 (continued)

Author	Methods used	Description
Singh et al. [19]	Energy efficient routing protocol with PSO for WSN	Compared to other approaches, PSO gives better result in cloud.
Izakian et al. [20]	Discrete PSO	In order to minimize the makespan and flow time, this approach used DPSO for job scheduling. Evaluation proves better result than other evolutionary algorithms such as GA and ACO.
Sarwar et al. [21]	Divide and Conquer privacy preserving approach	Derived data division strategy based on Level of privacy and transmits among the fog nodes for aggregation. This method reduces the computational cost, memory overhead and ensures the data privacy.

3 Proposed Discrete GWO Methodology

In this section, Fig. 1.Illustrates the proposed system overview of efficient Edge IoT enabled smart healthcare. This system supports patient health monitoring at distant location remotely. This system involves three kind of nodes such as Mobile node (MN), Aggregator node (AN) and Edge node (EN). Each wearable IoT sensor devices are the mobile nodes. Large number of these IoT device sensor nodes forms a cluster. Each cluster there is one node called AN aggregate all the data generated by MN and forward it into the base station/cloud centre through edge node. The data generated by MN are compressed and encrypted using ECE and add MAC to ensure the security of the data. This encrypted data is aggregated by AN using XOR operation of MAC with key. The AN nearer to edge node will transfer the aggregated data to edge server directly. In the case of AN which placed far wary from the edge server can communicate to its neighbor cluster AN for-message transmission. Neighbor AN can be find using optimization algorithm called Discrete GWO which will efficiently find the nearest neighbor for message transmission. Edge node received aggregated data from each cluster AN and decrypt the data for local processing to reduce the cloud server overhead then forward it into cloud server for central storage and analysis. Cloud data centre process the received data and transfer the analyzed results to respective authority for early diagnosis.

3.1 Data Encryption and Aggregation Using ECE-MAC

Wearable IoT sensor devices collect the health parameter and transmit it into AN. Data compression and ECE-MAC encryption is performed for effective data transmission between AN and EN. The data gathered by the sensor nodes are aggregated and compressed using the compression method. Aggregated data of health parameter is represented as $MN_{agg} = \{HP_1, HP_2, \ldots HP_n\}$ *where* $n \in [1, N]$, N-number of SN. This compress data is encrypted using ECE encryption. Elliptic Curve based Elgamal based privacy homomorphism encryption is an asymmetric cryptography approach. in this scheme, the encryption key is publicly known for AN and EN. The message is mapped into elliptic curve. The message is multiplied with the generator of EC. In decryption demap the point again to m. For mapping, brute force computation is used. ECE algorithm is as follows:

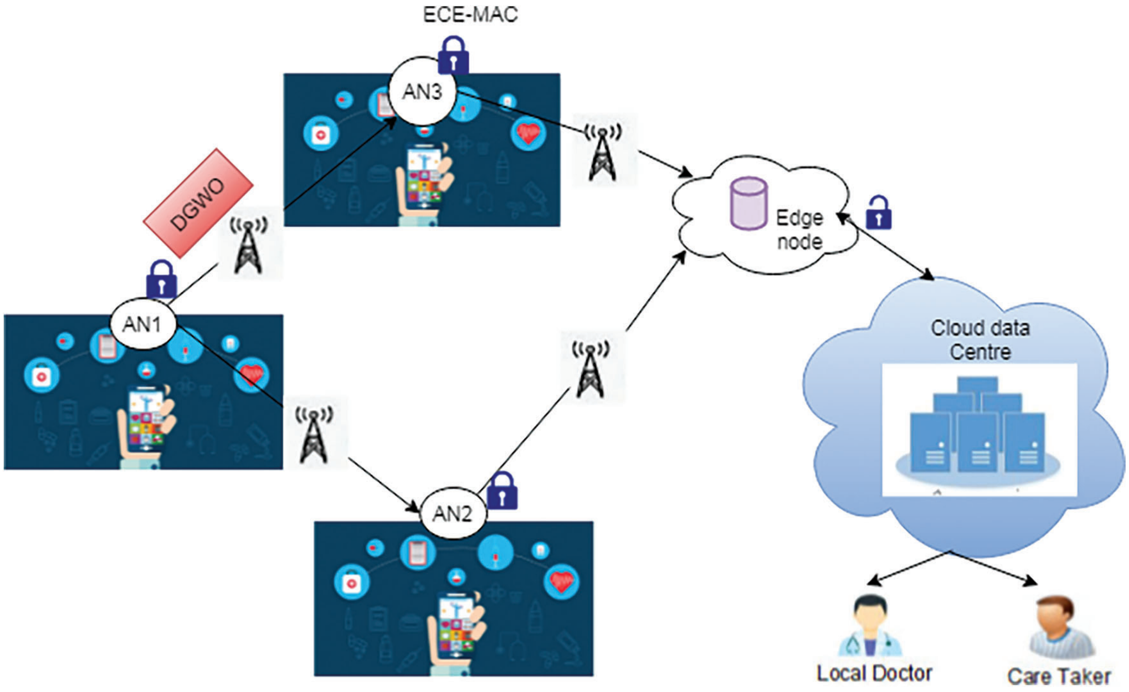

Figure 1: Overview of proposed smart healthcare system

Algorithm 1: (ECE and compression)

```
Step 1: Parameter Initialization: private key z (integer), public key (X, Y) X and Y are the points on EC where Y = zX.
Step 2 : Encryption $C = [c_1, c_2] = [kX, kY + mX] =$ EC points tuple (1)
Step 3 : Decryption $mX = (kY + mX) - z(kX)$and demap mX\right arrow m (2)
Step 4: Aggregation: EC- Scalar addition
$C_{agg} = [C_1, C_2] = (c_{11} + c_{21}), (c_{12}, c_{22})$ (3)
Step 5 : Compression $cd\_i = compr(C\_agg)$ (4)
```

Message authentication code (MAC) is a cryptographic construction that is used to identify the falsification of the messages. It is represented using one way hash function, secret key generated by ECE and the message of length t. This MAC will increase the integrity and the receiver needs to recalculate the MAC code with its decryption to ensures the authenticity using the Eq. (5).

$$MAC = Hash_k(t) \tag{5}$$

This MAC codes are aggregated with bitwise XOR operations, and the result enable authentic verification. The aggregated MAC is represented in Eq. (6)

$$MAC_{agg} = MAC_1 \otimes MAC_2 \otimes, \ldots \otimes MAC_n \tag{6}$$

Data integrity is preserved during aggregation by each node MAC is combined by XOR operation. The aggregated MAC is verified by EN and cloud server. The aggregated data are decrypted by EN based on the key and aggregated MAC. This proposed scheme will ensure the data confidentiality, data integrity and data authentication. Data confidentiality is ensured through secret key shared by the sensor node and AN. There is no adversary violation on aggregated data.

3.2 DGWO to Find Neighbor AN

This section discusses about the technique to find the nearest AN for message transmit if there is no peer-to-peer communication between edge node and AN. To find the best possible solution, this work implements grey wolf optimization approach with discrete weight. Grey wolfs are the advanced optimization algorithm depends on the hunting nature of the wolf that is ready to catch their prey because all are stayed in the crowd that are organized carefully [22]. The four levels of GWO leadership hierarchy are alpha (α), beta (β), delta (δ), and omega (ω). α is the male or female whose are the leaders for making decisions. β will help alpha to make decisions. δ are the guides or elders or hunters. ω follow all wolves and it will be outlasting solution whereas alpha, beta and omega are the first, second and third best solutions.

In this proposed work, for feature selection the labeled data are separated into two sets of positive and negative represented as matrix of PM and NM. Each row of these matrix represented as the recommended medical tests carried and each column represents that the result of these medical tests [23]. If the deviation between these two values is lower than threshold then the value obtained from the record will falls onto any of the label. So, the attributes are insignificant to determine the label. The values with no deviation between positive and negative label are stated as suboptimal one. Hence, need to select the attributes that representing the diversity observed in both positive and negative label.

In order to find the optimal attributes, this proposed work use DGWO to identify the diversity between the attributes and corresponding vector values of both positive and negative label. The aim of this phase is to select the relevant features that can increase the prediction accuracy. To start the optimization algorithm, initialization with the initial population is the first step. The alpha (α), beta (β) and delta (δ) are the three best possible solutions in the GWO. The outstanding solution is represented as omega. Throughout the hunting process, the wolf is surrounded by their prey which is represented as,

$$D = |E \times X_p - X_t| \tag{7}$$

$$X_{(t+1)} = |X_{p(t)} - A \times D| \tag{8}$$

$$E = 2 \times r1 \tag{9}$$

$$A = |2a \times r2 - a| \tag{10}$$

where,

X_p–Location of prey, X_t–location of the grey wolf, t- iteration, r1. r2–random vectors in the range [0, 1], a∈[0, 2] represented as,

$$a = 2 - t \times \frac{2}{Max.\ no\ of\ iterations} \tag{11}$$

The location of the grey wolf with optimal solution can be changed by modifying the coefficient vectors E and A. The alpha (α), beta (β), and delta (δ) are responsible for prey placements. The remaining wolves change their locations according to the best three solutions as,

$$\bar{X}_1 = X_\alpha - A_1 \times D_\alpha \tag{12}$$

$$\bar{X}_2 = X_\beta - A_2 \times D_\beta \tag{13}$$

$$\bar{X}_3 = X_\delta - A_3 \times D_\delta \tag{14}$$

$$X_{(t+1)} = \frac{\bar{X}_1 + \bar{X}_2 + \bar{X}_3}{3} \tag{15}$$

where,

$$D_\alpha = |E_1 \times X_\alpha - X| \tag{16}$$

$$D_\beta = |E_2 \times X_\beta - X| \tag{17}$$

$$D_\delta = |E_3 \times X_\delta - X| \tag{18}$$

The wolves are updated their position while attacking their prey between their current position and prey position when |A|<1. The optimal attributes are selected using this GWO. Now, the resultant matrices of PM and NM having the column values as the optimal solution selected by the GWO. These matrices used to find the n optimal AN. Move all the optimal attributes to the set of selected AN called nAN (number of selected AN set). The new subset of AN are formed by combining the two subsets of AN

$$x = x_i \cup_j^x \tag{19}$$

For each record

$$\forall_{i=1}^{n} \{x_i \exists x_i \ \in nAN\} \tag{20}$$

$$\forall_{j=1}^{n} \{x_j \exists x_j \ \in nAN \wedge j \neq i\} \tag{21}$$

The empirical property of these selected feature set is discovered for each selected attribute and calculate the positive and negative probability of empirical value as, $\forall_{i=1}^{nAN} \{nAN \exists nAN \in nAN\}$

$$\text{Positive label probability}\, pp_{nFS} = \frac{\sum_{i=1}^{nAN} \{1 \exists nAN \subseteq PM(k)\}}{|PM|} \tag{22}$$

$$\text{Negative label probability}\, np_{nFS} = \frac{\sum_{i=1}^{nAN} \{1 \exists nAN \subseteq NM(k)\}}{|NM|} \tag{23}$$

Based on the empirical value assign the ranks to the attributes in ascending order for positive and negative label accordingly. After assigning the ranks, normalization is performed by assigning local and global weights to positive and negative label as,

$$pw_{nAN} = 1 - (pgw \times plw) \tag{24}$$

$$nw_{nAN} = 1 - (ngw \times nlw) \tag{25}$$

The positive weights are updated by multiplying the global positive label weight with local weight and subtract the result with 1. And the same for negative label weights are calculated by multiplying the global and local weight of the negative label attributes and subtract it with one, which is the result value.

Algorithm 2: Neighbor AN finding using DGWO

```
Input: aggregated data, initial population X, max no of iterations tmax, size N, control parameter a
Output : optimal neighbor AN
Step 1:     for i = 1 to N
Step 2:         for j = 1 to d
Step 3: PM [i, j] = positive label records
        NM [I, j] = negative label records
Step 4:     end For
Step 5:end for
Step 6: for t = 1: tmax
Step 7:          update a using Eq. (9)
Step 8:     for i = 1:N
Step 9:     for j = 1:d
Step 10:         calculate $D_\alpha$, $D_\beta$, $D_\delta$ Eqs. (16)–(18)
Step 11:         calculate the probability and weights using Eqs. (20)–(23)
Step 12:         update the position using Eqs. (12)–(15)
Step 13:    end For
Step 14:    end For
Step 15:    end For
```

Now based on the weight's updates, the AN are ranked in ascending order. The AN having high values are considered as relevant AN for further message transmission towards EN.

4 Performance Analysis and Discussions

The proposed efficient data aggregation scheme for healthcare applications is simulated using NS2.35. Proposed system is evaluated in terms of functionality, communication cost and energy cost. Performance of the proposed system is compared with the existing approaches such as secure privacy preserving data aggregation scheme (SPPDA) [24], concealed data aggregation scheme for multiple application (CDAMA) and secure aggregation scheme (ASAS) [25]. The functionalities such as recoverability, data confidentiality, data authentication, data integrity and false data filtering [26–38] are used. The results are listed in Tab. 2.

4.1 Energy Efficiency

Energy in terms of three level such as SN, AN and EN are considered with the network size varies from 100 to 500 nodes [31–35]. Fig. 2. illustrates the energy cost of proposed and existing approaches in μJ. Energy cost for proposed system for 300 nodes is 0.34 μJ. Various energy of the existing approaches such as SPPDA, CDAMA and ASAS are 1.3 μJ, 0.81 μJ and 0.51 μJ respectively. From the evaluation, it is observed that proposed scheme consumes less energy than other existing approaches.

Table 2: Evaluation of proposed system functionality

Methods	Recoverability	Data confidentiality	Data authentication	Data integrity	False data filtering
SPPDA	Yes	Yes	No	Yes	No
CDAMA	No	Yes	No	Yes	Yes
ASAS	Yes	Yes	No	No	No
Proposed scheme	Yes	Yes	Yes	Yes	Yes

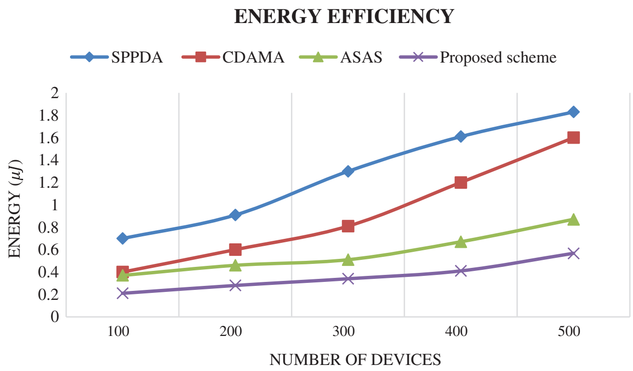

Figure 2: Energy efficiency comparison

4.2 Communication Cost

Evaluation based on cost of communication using proposed scheme is shown in Tab. 3. Execution time and energy cost in terms of SN, AN and EN. Execution time includes processing and aggregation time. Energy cost includes computation and aggregation cost. proposed scheme consumes 7.9mJ for sending a data per bit for 300 nodes and 9.3mJ for receiving data per bit. Performance of the proposed system cost is compared with existing approaches is shown in Fig. 3.

Table 3: Performance of proposed scheme

No of nodes		100	200	300	400	500
Aggregation time (s)		0.61	0.89	1.4	1.9	2.5
Aggregation energy cost (μJ)		0.34	0.39	4.2	4.8	5.1
Communication cost(mJ)	Send	6.3	7.2	7.9	8.4	8.9
	Receive	7.3	8.5	9.3	10.2	10.9

The evaluation of Fig. 3. shows that the minimum communication cost is obtained by proposed scheme. For 300 devices, the communication cost of proposed scheme is 17.84mJ. Various, existing approaches obtained 20.43mJ, 17.21mJ, and 18.92mJ for SPPDA, CDAMA and ASAS respectively.

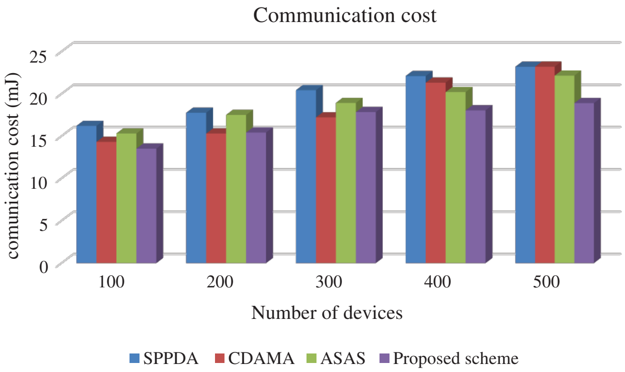

Figure 3: Comparison of communication cost

Proposed scheme obtained less energy cost and communication cost compared to other existing approaches. Due to the implementation of evolutionary algorithm to search the neighbor AN, and peer to peer communication between AN and EN, the messages are efficiently transfer to cloud server for processing. The encryption method used here is send the data confidentially through the network. Hence, proposed scheme is efficient and effective for transmitting the data collected from the sensor devices to cloud for processing and better diagnosis.

5 Conclusion

With the interconnection of IoT devices and digital technologies, smart healthcare ensures better human life. To transmit the sensitive health data through WSN is a challenging task. This paper proposed a secure data transmission of healthcare data through WSN using data aggregation with evolutionary approaches for better diagnosis. This model ensures the security of the data by avoiding several attacks using ECE-MAC approach. Data gathered from sensor devices are aggregated and transfer to EN which is the mediator of AN and cloud. If there is no peer-to-peer communication means, AN sends data to its neighbor AN using DGWO approach. This will reduce the transmission cost and energy. This proposed model is secured with less energy of 0.34 μJ to transfer data from 300 devices and obtained 17.84mJ as communication cost for 300 devices. Compared to conventional approaches such as SPPDA, CDAMA and ASAS, proposed scheme ensures data confidentiality, data integrity, data authentication and false data filtering. In future, proposed scheme is simulated on particular disease diagnosis with secure data transmission.

Funding Statement: This research was supported by a grant of the Korea Health Technology R & D Project through the Korea Health Industry Development Institute (KHIDI), funded by the Ministry of Health & Welfare, Republic of Korea (grant number: HI21C1831) and the Soonchunhyang University Research Fund.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. M. Farhan, N. Scarpato, A. Pieroni, L. D. Nunzio and F. Fallucchi, "E-Health-IoT universe: A review, " *International Journal on Advanced Science, Engineering and Information Technology*, vol. 7, no. 6, pp. 2328, 2017.

[2] M. Aazam, S. Zeadally and K. A. Harras, "Fog computing architecture, evaluation, and future research directions," *IEEE Communications Magazine*, vol. 56, no. 5, pp. 46–52, 2018.

[3] M. M. Dhanvijay and S. C. Patil, "Internet of things: A survey of enabling technologies in healthcare and its applications," *Computer Network*, vol. 153, pp. 113–131, 2019.

[4] J. N. S. Rubí and P. R. L. Gondim, "IoMT platform for pervasive healthcare data aggregation, processing, and sharing based on one M2 M and open EHR," *Sensors*, vol. 19, no. 19, pp. 4283, 2019.

[5] A. Gatouillat, Y. Badr, B. Massot and E. Sejdic, "Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine," *IEEE Internet Things*, vol. 5, no. 5, pp. 3810–3822, 2018.

[6] M. Usak, M. Kubiatko, M. S. Shabbir, O. V. Dudnik, K. Jermsittiparsert *et al.,* "Health care service delivery based on the internet of things: A systematic and comprehensive study," *International Journal of Communication Systems*, vol. 33, no. 2, pp. 12–34, 2020.

[7] H. Wang, Z. Wang and J. Domingo Ferrer, "Anonymous and secure aggregation scheme in fog-based public cloud computing," *Future Generation Computer System*, vol. 78, pp. 712–719, 2018.

[8] A. Ullah, G. Said, M. Sher and H. Ning, "Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN," *Peer-Peer Network Application*, vol. 13, no. 1, pp. 163–174, 2020.

[9] H. Zhu, L. Gao and H. Li, "Secure and privacy-preserving body sensor data collection and query scheme," *Sensors*, vol. 16, no. 2, pp. 1–16, 2016.

[10] W. He, X. Liu, H. Nguyen, K. Nahrstedt and T. Abdelzaher, "Pda: Privacy-preserving data aggregation in wireless sensor networks," in *Proc. INFOCOM, 26th IEEE Int. Conf. on Computer Communications*, Anchorage, USA, pp. 2045–2053, 2007.

[11] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant *et al.,* "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Generation Computer System*, vol. 78, no. 3, pp. 659–676, 2018.

[12] C. Gosman, C. Dobre and F. Pop, "Privacy-preserving data aggregation in intelligent transportation systems," in *Proc. IEEE Symp. on Integrated Network and Service Management*, Lisbon, Portugal, pp. 1059–1064, 2017.

[13] M. Azeem, A. Ullah, H. Ashraf, N. Z. Jhanjhi, M. Humayun *et al.,* "Fog oriented secure and lightweight data aggregation in IoMT," *IEEE Access*, vol. 9, pp. 111072–111082, 2021.

[14] Y. H. Lin, S. Y. Chang and H. M. Sun, "CDAMA: Concealed data aggregation scheme for multiple applications in wireless sensor networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 7, pp. 1471–1483, 2013.

[15] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun *et al.,* "Secure healthcare data aggregation and transmission in IoT,A survey," *IEEE Access*, vol. 9, pp. 16849–16865, 2021.

[16] C. M. Chen, Y. H. Lin and Y. C. Lin, "RCDA: Recoverable concealed data aggregation for data integrity in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 4, pp. 727–734, 2012.

[17] A. Salman, I. Ahmad and S. Al Madani, "Particle swarm optimization for task assignment problem," *Microprocessors and Microsystems*, vol. 26, no.8, pp. 363–371, 2002.

[18] K. A. Shim and C. M. Park, "A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 8, pp. 2128–2139, 2015.

[19] A. Singh, S. Rathkanthiwar and S. Kakde, "Energy efficient routing of WSN using particle swarm optimization and V-LEACH protocol," in *Proc. Int. Conf. on Communication and Signal Processing (ICCSP)*, Melmaruvathur, India, pp. 15–34, 2016.

[20] H. Izakian, B. T. Ladani, A. Abraham and V. Snel, "A discrete particle swarm optimization approach for grid job scheduling," *International Journal of Innovative Computing*," *Information and Control*, vol. 6, no. 9, pp. 1–15, 2010.

[21] K. Sarwar, S. Yongchareon, J. Yu and S. Rehman, "Lightweight, divide-and-conquer privacy-preserving data aggregation in fog computing," *Future Generation Computer Systems*, vol. 119, no. 2, pp. 188–199, 2021.

[22] I. M. Easnony, S. I. Barakat, M. Elhoseny and R. R. Mostafa, "Improved feature selection model for big data analytics," *IEEE Access*, vol. 8, pp. 66989–67004, 2020.

[23] M. A. Yarimi, N. M. Munassar, M. Bamashmos and M. Ali, "Feature optimization by discrete weights for heart disease prediction using supervised learning," *Soft Computing*, vol. 2, no. 3, pp. 1–15, 2020.

[24] C. Zhang, C. Li and J. Zhang,“A secure privacy-preserving data aggregation model in wearable wireless sensor networks,” *Journal of Electrical and Computer Engineering*, vol. 61, no. 3, pp. 1–9, 2015.

[25] H. Wang, Z. Wang and J. Ferrer, “Anonymous and secure aggregation scheme in fog-based public cloud computing,” *Future Generation Computer System*, vol. 78, no. 3, pp. 712–719, 2018.

[26] M. Abdel Basset, D. E. Shahat, K. Deb and M. Abouhawwash, “Energy-aware whale optimization algorithm for real-time task scheduling in multiprocessor systems,” *Applied Soft Computing*, vol. 93, p.1 06349, 2020.

[27] M. Abdel Basset, R. Mohamed, M. Abouhawwash, K. Ripon Chakrabortty and J. Michael, “EA-MSCA: An effective energy-aware multi-objective modified sine-cosine algorithm for real-time task scheduling in multiprocessor systems: Methods and analysis,” *Expert Systems with Applications*, vol. 173, pp. 114699, 2021.

[28] M. AbdelBasset, R. Mohamed and M. Abouhawwash, “Balanced multi-objective optimization algorithm using improvement based reference points approach,” *Swarm and Evolutionary Computation*, vol. 60, pp. 100791, 2021.

[29] H. Seada, M. Abouhawwash and K. Deb, “Multiphase balance of diversity and convergence in multiobjective optimization,” *IEEE Transactions on Evolutionary Computation*, vol. 23, no. 3, pp. 503–513, 2019.

[30] M. Abouhawwash and A. M. Alessio, “Multi objective evolutionary algorithm for PET image reconstruction: Concept,” *IEEE Transactions on Medical Imaging*, vol. 40, no. 8, pp. 2142–2151, 2021.

[31] N. S. Murugan, D. G. gopal, U. Kumaran, M. Thirunavukkarasan, M. D. Alshehri *et al.,* “Secure data transmission in internet of medical things using RES-256 algorithm,” *IEEE Transactions on Industrial Informatics*, vol. 6, no. 2, pp. 1–14, 2021.

[32] M. Abouhawwash, “Hybrid evolutionary multi-objective optimization algorithm for helping multi-criterion decision makers,” *International Journal of Management Science and Engineering Management*, vol. 16, no. 2, pp. 94–106, 2021.

[33] G. G. Deverajan, V. Muthukumaran, C. H. Karuppiah and M. Chung, “Public key encryption with equality test for industrial internet of things system in cloud computing,” *Transactions on Emerging Telecommunications Technologies*, vol. 17, no. 3, pp. e4202, 2021.

[34] G. G. Deverajan and R. Saravanan, “Selfish node detection based on evidence by trust authority and selfish replica allocation in DANET,” *International Journal of Information and Communication Technology*, vol. 9, no. 4, pp. 473–491, 2016.

[35] M. Abouhawwash and K. Deb, “Reference point based evolutionary multi-objective optimization algorithms with convergence properties using KKTPM and ASF metrics,” *Journal of Heuristics*, vol. 27, no. 12, pp. 575–614, 2021.

[36] S. M. Nagarajan, G. G. Deverajan, P. Chatterjee, W. Alnumay and U. Ghosh, “Effective task scheduling algorithm with deep learning for internet of health things (IoHT) in sustainable smart cities,” *Sustainable Cities and Society*, vol. 71, pp. 102945, 2021.

[37] M. Abouhawwash, K. Deb and A. Alessio, “Exploration of multi-objective optimization with genetic algorithms for PET image reconstruction.”, *Journal of Nuclear Medicine*, vol. 61, no. 4, pp. 572–572, 2020.

[38] D. Rao, S. Huang, Z. Jiang, G. G. Deverajan and R. Patan, “A dual deep neural network with phrase structure and attention mechanism for sentiment analysis,” *Neural Computing and Applications*, vol. 33, pp. 11297–11308, 2021.